JUDGE ROBERT J. BRYAN

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT TACOMA

UNITED STATES OF AMERICA, Plaintiff, v. JAY MICHAUD, Defendant.	No. CR15-5351RJB REPLY TO GOVERNMENT'S RESPONSE TO MOTION TO VACATE AND RESPONSE TO GOVERNMENT MOTION FOR IN CAMERA REVIEW

I. INTRODUCTION

As the Court is aware, the Government has offered two specific justifications for the protective order. The first is that public disclosure of the protected material could jeopardize continuing investigations by "identifying the true name of Website A." *See* Stipulated Motion for Entry of Discovery Protective Order (Dkt. 17) at 2. The defense has recently learned, however, that the Government has already revealed the actual name of "Website A" and details of the current NIT program in connection with other recent cases, and that these disclosures have been the subject of news reports in other jurisdictions and online. Under these circumstances, the Government has effectively waived any claim that the site's name or the FBI's NIT capabilities are confidential or that modification of the discovery restrictions in this case will compromise pending investigations.

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

Moreover, as noted in the Motion to Vacate, the defense has no objection to redacting the name of the site from discovery that is publicly filed as exhibits, or shared with attorneys or organizations that are not part of the defense team. *See* Motion to Vacate (Dkt. 32) at 4-5.[1] Nor does the defense object to a revised and limited protective order that covers any new discovery that contains the site's name. The bulk of the investigation reports, warrants and warrant applications, and other discovery that the Government has designated as "protected" make no mention of the site's actual name, and segregating the records that do will be a simple matter. The Government makes no effort to explain why these more focused protections are not sufficient to address any legitimate interest it may have in preventing further publicity about the site.[2]

Second, the Government has alleged that a protective order is needed because disclosure would expose "sensitive investigative techniques." Govt. Reply at 9. Here again, the defense has no objection to a narrowly tailored protective order for discovery that contains information about the "Network Investigative Technique" which has not already been made public, such as its programming code (which the Government has so far refused to disclose). The problem for the Government is that the summary information about the NIT that is in the discovery and referenced in the Motion to Suppress is already public, and in fact almost all this public information came from the

---

[1] The Government notes that the defense offered to adopt reasonable redactions for the motion to suppress in an effort to resolve any objections to unsealing the pleading, but the defense rejected the proposed redactions. *See* Govt. Reply at 11-12. Given that the Government's proposed edits encompassed the bulk of the motion and rendered it virtually unreadable, it should have come as no surprise that Mr. Michaud has elected to proceed with the motion to vacate and unseal.

[2] The Government produced discovery containing the name of the site for the first time on October 29, more than three months after the defense served its omnibus discovery demands and after the motion to vacate was filed on October 20. This discovery consists of several screen shots and a disc of data recovered from the site. A defense expert has also received mirror image copies of Mr. Michaud's data storage devices for forensic analysis, and the agreed procedures for handling that data are not disputed.

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

Government itself. *See* § B, *infra*. Obviously, it makes no sense for the Government to insist that disclosure of the NIT information in the discovery would reveal confidential "methods" (*see* Govt. reply at 7) when it has already disclosed those methods elsewhere and in more detail.

Instead of addressing the discrepancy between the representations in its pleadings about the need for confidentiality and the fact that it has already disclosed the information at issue, the Government offers nothing more than broad claims that vacating the order will "jeopardize" the investigation of other users of "Website A." *See, e.g*, Govt. Reply at 4. As discussed in more detail below, the Government is hard pressed to make these claims, when it has previously asserted that users would likely be alerted to an investigation as soon as the site was shut down, which happened more than nine months ago (*see* Motion to Vacate at 5); the Government has already publicly disclosed the name of the site and its NIT methods; and any target user capable of finding the site on the Tor network is equally capable of "Googling" the site's name and finding the Government's disclosures and the related news reports.

Given these facts, and the fact that the Government does not seriously dispute the presumption against protective and sealing orders or the need to show "with specificity" good cause for limiting access to trial records (*see* Motion to Vacate at 2-4), the Court should find that the Government has failed to meet its burden and vacate or modify the protective and sealing orders accordingly. *Compare, e.g., United States v. Chow*, No. CR 14-00196, 2014 WL 2093488 (N.D. Cal, May 19, 2014) (good cause for protective order limiting disclosure of the identities of undercover agents when Government established that they could be harmed if their names became public) (cited in Govt. Reply at 7).

Further, while the defense is not required to show a particularized need in opposing prosecution efforts to keep court records and proceedings secret, there is in

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

fact a pressing need to lift the veil the Government has haphazardly tried to cast over its surveillance methods. As noted in the Motion to Vacate, the defense is seeking changes in the disclosure rules because they are hampering its ability to communicate and coordinate with other defense counsel and public interest organizations in responding to an extraordinary expansion of Government surveillance and its use of illegal search methods on a massive scale.

In this regard, the Government has recently filed charges based on its investigation of "Website A" in numerous states, including Connecticut, Massachusetts, Illinois, New York, New Jersey, Florida, Utah, and Wisconsin. All the "Website A" cases are being supervised and coordinated by the Child Exploitation and Obscenity Section (CEOS) of DOJ's criminal division. As a result, the defense's discovery requests and pleadings in this case have been forwarded by the U.S. Attorney's Office to CEOS for review, and an attorney from that office has entered a notice of appearance in this case.[3] The Government's attorneys are able freely to strategize, share and discuss the warrants and other evidence, and review, edit and circulate pleadings. At the same time, the Government has gone so far as to object to the defense sharing copies of its motion to suppress evidence with other attorneys who are litigating "Website A" cases, on the ground that it references facts in the Title III and NIT warrants. This is so even though the facts summarized in the pleading are not only already known to all the attorneys working on these cases, but also are public. It therefore appears that the Government is using protective and sealing orders more as a

[3]AUSA Kate Vaughn remains the line prosecutor in this case and is not affiliated with CEOS. It also appears that she had no role in the "Website A" investigation, nor is there any indication that she is involved in the related cases pending in other districts or was personally aware of the disclosures that DOJ made in some of those cases. However, the Government's response to the motion to vacate was reviewed and approved by CEOS.

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

tactical means to divide and conquer defendants than to preserve any legitimate confidentiality interests.[4]

Finally, in an apparent effort to patch the holes in its response, the Government seeks permission to file an "in camera" letter with the Court, ostensibly to provide "further evidence of why vacating or modifying the protective order" would jeopardize ongoing investigations. Govt. Motion for In Camera Review at 1. This extraordinary request is really an attempt to engage in improper ex parte communications with the Court and it should be summarily denied. If there is additional information which bears on the pending motion that the Government believes is both relevant and sensitive, it can submit that information under seal or seek an independent protective order for it. The Government offers no justification for concealing its communications with the Court from the defense or preventing the defense from responding to its "letter."

II. ARGUMENT

A. The Site is Not Named in Most of the "Protected" Discovery or the Motion to Suppress and, in any event, the Government Itself Has Disclosed the Name in Other Proceedings.

The actual name of "Website A" is not mentioned anywhere in the Motion to Suppress or accompanying exhibits, including the Title III and NIT warrants and applications, which are the key records in terms of joint defense preparations. Instead, the motion and relevant discovery refer to "Website A" or "Target Website" throughout. The Government, however, ignores the discrepancy between its purported need to keep the name of the site confidential and the fact that the name does not appear in the

[4] While the Government recognizes that the protective order does not prevent Mr. Michaud from retaining individual experts affiliated with the ACLU or other organizations (*see* Govt. Response at 10), it does prevent those experts from sharing basic factual information about the NIT cases with their parent organizations and the board members who would decide whether to seek permission from the Court to appear as *amici*. Consequently, defense efforts to enlist the support of the ACLU and other interested public interest groups have largely stalled.

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

pleading and records at issue, and instead relies on generic justifications for continued secrecy. *See, e.g.,* Govt. Reply at 4 ("public disclosure of sensitive discovery materials in this case is likely to jeopardize [the] ongoing investigation."). To make matters worse, the Government has not alerted the Court to the fact that it has already revealed the name of "Website A" in other pleadings.

On September 23, 2015, the Government filed an unsealed complaint in the Eastern District of New York which includes the actual name of "Website A." The details of that complaint (including the name) were published in local news reports and on numerous online news sites. *See* Sealed Affidavit of Colin Fieman in Support of Motion to Vacate (Fieman Aff.), exh A at ¶ 20 (publicly filed complaint identifying "Website A"); exh. B (related news reports naming the website). The defense recently found this complaint and the related media reports simply by "Googling" the actual name of "Website A" and then downloading a copy of the complaint from public court records. Other recent news reports have provided detailed accounts of the "Website A" investigation and the Government's use of an NIT in connection with it. While these additional reports do not disclose the name of the site, they include all of the other identifying information about the site (such as the date it was seized, the location of its server, and the number of its members) that is contained in the discovery. *See* Fieman Aff., exhs. C and D.[5]

In short, the Government cannot credibly maintain that the protective order is needed to avoid publicizing the name of the target site, when the motion to suppress and related discovery do not include that name and the Government has already disclosed it.

---

[5]The defense maintains that filing this information under seal is unnecessary, since the exhibits consist of public documents and news reports, and also inconsistent with the public's right to access court proceedings and Mr. Michaud's right to a public trial. However, until the Court provides further guidance on this issue, the defense will continue to err on the side of caution and submit exhibits naming the site under seal.

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

If the Court deems it appropriate, the defense has no objection to continuing to refer to the site as "Website A" or the "Target Website" in its public filings.

B. The Government's "Network Investigative Technique" Has Also Been Widely Disclosed and the Protected Discovery Does Not Contain Any New Information About the NIT.

The Government also maintains that there is good cause to keep the motion to suppress sealed and restrict the sharing of information about the Title III and NIT warrant applications because the "particular investigative technique[]" is secret, it is "described in detail," and disclosure will undermine pending investigations. *See* Govt. Reply, *e.g.*, at 9. All of these claims are nonsense.

First, it is important to note that the motion and related discovery contain nothing more than general summaries of what the NIT does and the type of information it extracts from target computers. *See* Defendant's Motion to Suppress, exh. C at ¶¶ 31-37 (Dkt. 26). As previously noted, the Government has not disclosed any detailed technical information about the NIT, such as its programming code. The Government has in fact declined to disclose the code, even though the defense has offered to enter into a separate protective order for any details about the NIT for which there are legitimate confidentiality concerns. The Government has not responded to this offer.[6]

Further, all of the information in the discovery about how an NIT infiltrates target computers and the type of information it extracts has previously been disclosed by the Government in far greater detail in other NIT cases. *See* Motion to Vacate, exhs. A and B (records filed in *United States* v. *Cottom et al,* CR-13-108 (D. Neb.)).[7] In

---

[6] The Government's refusal to provide this and other discovery will be the subject of a separate motion to compel discovery.

[7] The Government notes that it objected to the public filing of the NIT disclosures in *Cottom* and asked the Nebraska court to place those disclosures under seal. Govt. Memo at 9, n 5. The fact that the court found that the disclosures should remain public and denied the request to seal hardly helps the Government in this case. In addition, the *Cottom* court did not,

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

response, the Government asserts that the NIT used in the Nebraska cases is different because it "was publicly-sourced" and is "no longer in use." Govt. Reply at 9. This is like saying wiretapping should be considered a secret investigative technique because the Government may use different recording devices in different cases. The point is that the Government's ability to surreptitiously extract IP addresses from target computers on "the dark web" is already public information, and there is no new information or technical details in the protected discovery that adds to what it has been disclosed in other cases about this investigative capability.

In addition, there have been several detailed articles about the FBI's NIT capabilities that go into far more detail than the summaries contained in the protected discovery. For example, more than a year ago, JustSecurity.Org, an online news service for cyber security businesses and experts, published a report on NIT's and how they work, including the following explanation:

> Broadly, the term "Network Investigative Techniques," (NIT) describes a method of surveillance that entails "hacking," or the remote access of a computer to install malicious software without the knowledge or permission of the owner/operator. Once installed, malware controls the target computer. The right Network Investigative Technique can cause a computer to perform any task the computer is capable of—covertly upload files, photographs and stored e-mails to an FBI controlled server, use a computer's camera or microphone to gather images and sound at any time the FBI chooses, or even take over computers which associate with the target (e.g. by accessing a website hosted on a server the FBI secretly controls and has programmed to infect any computer that accesses it). Network Investigative Techniques are especially handy in the pursuit of targets on the anonymous Internet—defined for the purposes of this post as those using Tor, a popular and robust privacy software, in order to obscure their location (and other identifying information), and to utilize so-called "hidden" websites on servers whose physical locations are theoretically

---

as the Government suggests,"ultimately den[y] all the defendants' motions to suppress pertaining to the investigative technique." *Id.* In fact, for reasons that are unclear, the only ground for suppression raised by the Nebraska defendants was violation of Rule 41's notice provisions.

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

> untraceable. Since Network Investigative Techniques work by sending surveillance software over the Internet, the physical location of the target computer is not essential to the execution of the search.

Ahmed Ghappour, *Justice Proposal Would Massively Expand FBI Extraterritorial Surveillance*, JustSecurity.org (September 16, 2014) (also discussing the Government's so far unsuccessful efforts to amend Fed R. Crim P. 41(b) to allow for warrants to search computers outside the district where the warrant is issued).[8]

If all this public information about NIT's did not put to rest any further claim by the Government that its use of such malware is confidential, DOJ itself has made disclosures in pending NIT cases that directly undermine that claim. On July 6, 2015, the Government moved to unseal a June 10, 2015, search warrant and application in *United States v. Ferrell*, CR15-331 (E.D.N.Y.) (the original warrant application was filed under case number 15-M-0534). *See* exh. A (attached hereto) ("The *Ferrell* Application"). All of the information related to "Website A" and its use of an NIT that the Government claims cannot be disclosed without jeopardizing pending investigations was in fact disclosed *at the Government's request* several months ago. *Compare, e.g., Ferrell* application at ¶¶ 4-18 (describing the target website in detail, including its location and contents) *with* Defendant's Motion to Suppress, exh. B at ¶¶ 18-28 and exh. C at ¶¶ 11-27 (Dkt. 29); *Ferrell* application at ¶¶ 19-22 ("Court Authorized Use of Network Investigative Technique") *with* Motion to Suppress, exh. B at ¶ 53 and exh. C at ¶¶ 31-38; *see also* Nate Raymond, *Two People in N.Y. Charged in Massive Probe of Child Porn Website*, Reuters.com (July 8, 2015) (reporting on the unsealing of the *Ferrell* application and details of the "Website A" investigation).[9]

In addition, the Government filed another "Website A"/NIT case in the Southern District of Texas on June 5, 2015. During a preliminary hearing in that case on June 10,

---

[8]Available at: https://www.justsecurity.org/15018/justice-department-proposal-massive-expand-fbi-extraterritorial-surveillance/

[9]Available at: http://www.reuters.com/article/2015/07/08/usa-crime-childporn-idUSL1N0ZO1Y320150708#wKzxiStGEUCoEmDg.97

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

2015, FBI Special Agent Kelly Berry testified about the "Website A" investigation, the FBI's efforts to penetrate user anonymity on the "dark web," and its deployment of the NIT to extract identifying information from target computers. Exh. B at 3-5 (Transcript of June 10, 2015 hearing in *United States v. Hughes*, CR15-11 (S.D. Tx)). The Government did not ask the court to close the hearing or seal the transcript. Instead, the FBI issued a press release the same day about the case and the defendant's arrest was widely reported. These reports included details about the FBI's use of the NIT in connection with "Website A." *See, e.g.,* exh. C (summary of Orlando 6 TV News segment titled "FBI has New Tactic to Fight Child Pornography;" the broadcast version (link below) contains audio excerpts of Agent Kelly's testimony about deployment of the NIT).[10] It appears that, at the time, the Government preferred to tout its arrest of Dr. Hughes and publicize its NIT methods, perhaps as a deterrent to others who might seek out illicit content on the "dark web." Whatever the reasons, it is plainly inappropriate for the Government to disclose "protected information" when it suits its purposes, only to impede and resist the sharing and disclosure of the same information by defense counsel.

It is of course possible that these disclosures, and the Government's failure to inform the Court about them, happened because DOJ's left hand did not know what its right hand was doing. However, as already noted, the "Website A" investigation and the ensuing prosecutions of its users are being supervised and coordinated by CEOS. Given this chain of coordination and command, the Government's failure to acknowledge that it has already disclosed both "Website A's" name and its NIT capabilities suggests either a lack of diligence on DOJ's part in tracking its disclosures (which is inconsistent with its claim that these disclosures are "highly sensitive") or a lack of candor with the Court about the fact that the information it is seeking to withhold from closer public scrutiny has already been widely disseminated. Regardless

[10] Available at: http://www.clickorlando.com/news/fbi-has-new-tactic-to-fight-child-pornography/36069636. Other televisions stations in major metropolitan areas broadcast the same information; *see, e.g,.* http://www.click2houston.com/news/fbi-has-new-tactic-to-fight-child-pornography/35674978 (Houston's Channel 2 news).

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

of the explanation, the Government cannot credibly maintain that the information at issue is "highly sensitive" or confidential.

C. The Court has Broad Authority to Modify the Protective Order and Unseal Records.

Having failed to meet its burden of showing good cause for continuation of the Court's protective and sealing orders, the Government baldly asserts that this Court has no authority to vacate or modify its orders because the Title III and NIT warrants and applications were originally sealed in the Eastern District of Virginia. *See* Govt. Response at 11. The Government cites no authority for this argument, and the defense has been unable to find any rule or decision which limits a trial court's authority to make records public once they have been introduced as evidence in new proceedings pending before it. Moreover, Fed. R. Crim. P. 16(d)(1) grants the Court broad powers to regulate disclosures, and "at any time the court may, for good cause, deny, restrict, or defer discovery or disclosure, or *grant other appropriate relief*" (emphasis added). *See also* Fed. R. Crim. P. 16(d)(2) (authorizing courts to "enter…any order that is just under the circumstances" when overseeing discovery and the implementation of protective orders).[11]

A brief review of the sequence of events in this case amply demonstrates that vacating or modifying the protective order and unsealing the motion to suppress is appropriate. First, the Government asked the court in the Eastern District of Virginia to seal the Title III and NIT warrants and applications on the ground that disclosure of the

---

[11]The defense proposed to the Government that the parties file a joint motion to revise the E.D. Va. sealing orders in a way that would accommodate any legitimate confidentiality concerns, while at the same time ensure that those orders are not used as a pretext for blocking the dissemination of information that is already public or impeding communications between defense attorneys. The Government's response to that offer was unworkable and in fact sought to impose new restrictions on the defense.

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

information contained in those records would undermine its investigations. Then, on August 10, the Government moved for a protective order in this Court, on the ground that "further dissemination" of the warrants and other discovery would "seriously jeopardize" the Website A investigations and "reveal highly sensitive investigative techniques." Motion for Protective Order (Dkt. 17) at 2. The Government made this request despite its unsealing of the *Ferrell* application the preceding month; the public and widely reported testimony of FBI Agent Berry in June, 2015; and all the information about the FBI's NIT capabilities that had been circulating since 2013. Finally, after obtaining a protective order, the Government proceeded to disclose both the actual name of Website A and additional details about its NIT capabilities in the September 23 New York complaint. Given these facts, the best that can be said of the Government's representations in both the motion for protective order and reply to Mr. Michaud's motion is that they have been careless, if not affirmatively misleading.

Taking all these facts into consideration, as well as the broad powers afforded the Court under Rule 16 to vacate or modify protective and sealing orders, the Court should take appropriate measures to ensure that the defense can freely consult and coordinate with other defense counsel and public interest organizations on Mr. Michaud's behalf. At a minimum, these measures should include unsealing the Motion to Suppress; issuing a revised protective order that allows the defense to share all pleadings and discovery with other defense teams litigating NIT cases; and also allowing the defense to share its pleadings and copies of the Title III and NIT warrants and applications with organizations that advocate on behalf of the general public's privacy interests and constitutional rights.

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

D. The Government's Motion for "In Camera" Review of a Letter Should be Denied.

In conjunction with its reply to the motion to the vacate, the Government has filed a Motion for In Camera Review of a "letter" that will ostensibly provide "further evidence of why vacating or modifying the stipulated Protective Order would seriously jeopardize the ongoing investigation" of targets associated with "Website A." Govt. Motion for In Camera Review at 1. This motion should be denied.

It is one thing for a court to examine materials in camera when there is a question about whether those materials are relevant to the pending case and should be disclosed to the defense. Typically, in camera review occurs in situations such as a discovery demand for police personnel records or disclosure of confidential informant files. In those cases, there are specific and competing privacy interests or witness safety concerns that justify in camera review of pre-existing records that may or may not be relevant to the defense.

The situation here is altogether different. The Government is asking to submit a letter expanding on facts and arguments that are properly submitted as part of its responsive pleadings. As a result, what the Government is really proposing is an opportunity to engage in ex parte communications about the merits of maintaining a broad protective order, rather than in camera review of pre-existing records that may not even be relevant or discoverable.

The Ninth Circuit has repeated several times that "absent some 'compelling justification,' ex parte communications will not be tolerated," and that "ex parte proceedings are anathema in our system of justice." *Guenther v. Comm'r*, 889 F.2d 882, 884 (9th Cir. 1989), quoting *United States v. Thompson*, 827 F.2d 1254, 1258-59 (9th Cir. 1987). Surprisingly, the Government quoted *Thompson* as if it endorsed in camera review whenever a party claims that it needs "to keep sensitive information from the

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

opposing party." Govt. Motion for In Camera Review at 2. In fact, in *Thompson*, the Ninth Circuit reversed a district court's decision to receive in camera submissions (in that case, regarding a challenge to peremptory challenges under *Batson*). The court in no way endorsed what the Government seeks here.

More specifically, in *Thompson* the court began by noting two competing principles: "the district judge has broad discretion to fashion and guide the procedures to be followed in cases before him," but "adversary proceedings are the norm in our system of criminal justice, and ex parte proceedings the disfavored exception." *Id.* at 1257 (citation omitted). The court's "deference is not without limits[.]" *Id.* at 1258. For example, "[a] district judge may not adopt procedures that impair a defendant's right to due process or his other rights guaranteed by the constitution." *Id.* As to those rights, "[t]he right of a criminal defendant to an adversary proceeding is fundamental to our system of justice," including "the right to be personally present and to be represented by counsel at critical stages during the course of the prosecution." *Id.*

The *Thompson* court further explained that the defendant's right to participate is "not mere idle formalism. Our system is grounded on the notion that truth will most likely be served if the decision maker—judge or jury—has the benefit of forceful argument by both sides." *Id.* "Our judges usually have neither the time, nor the means, nor the training to investigate facts pertaining to the cases before them. Even on matters of law, our judges must rely heavily on counsel to come up with the arguments and citations supporting their respective positions." *Id.*

The court then cited various "occasional departures from this norm." *Id.* Each of the examples cited by the court fell into the first category discussed above, where the material reviewed in camera was the very material the defense sought (such as *Brady* material or facts about a confidential informant). It was in this context that the court referred to a need "to keep sensitive information from the opposing party." *Id.* Thus,

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

Thompson is not an endorsement of a free-floating exception to adversarial proceedings just because one party wants to submit information to the court and has a wish, or even a strong need, to keep that information secret.

The Government also cites to *Meridian Int'l Logistics, Inc. v. United States*, 939 F.2d 740 (9th Cir. 1991), a case dealing with certification that a civil defendant was acting in the course of his employment for purposes of the Federal Employees Liability Reform and Tort Compensation Act, 28 U.S.C. § 2679. *See* Motion for In Camera Review at 1. The district court allowed the Government to present an ex parte declaration regarding the defendant, an FBI agent. The Ninth Circuit upheld the court's consideration of ex parte materials, but first observed that "in our judicial system adversary proceedings are the norm and ex parte proceedings the exception[.]" *Id.* at 745. It also stated that "because procedures such as these should be used only in unique situations, we are careful to limit our holding to the precise facts of this case." *Id.* Given that the Ninth Circuit went on to reverse the district court's decision that the Government's submission was sufficient to determine whether the defendant was acting in the scope of his employment, the case in fact illustrates the danger of relying on ex parte communications. *Id*; *see also Wang v. United States*, 947 F.2d 1400, 1402 (9th Cir. 1991) ("The unavoidable implication of our decision in *Meridian International* is that, absent extraordinary circumstances," the court should not allow ex parte procedures).

In this case, the Government has made no showing about why it should be allowed to communicate with the Court ex parte, apart from boilerplate assertions that disclosure of its "letter" would "jeopardize" ongoing investigations. *See* Motion for In Camera Review at 1. The Court should find these statements insufficient to warrant the extraordinary step the Government is seeking. This is especially true given that the Government offers no explanation of why, even if the proposed letter contains sensitive

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

information, its submission under seal or pursuant to an independent protective order would not be sufficient to address any legitimate confidentiality concerns.

Accordingly, the Court should deny the Government's motion for in camera review.

DATED this 12th day of November, 2015.

Respectfully submitted,

s/ *Colin Fieman*
s/ Linda Sullivan
s/ Alan Zarky
Attorneys for Jay Michaud

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

CERTIFICATE OF SERVICE

I hereby certify that on November 13, 2015, I electronically filed the foregoing Reply to Government Response to Motion to Vacate Protective Order with the Clerk of the Court using the CM/ECF system, which will send notification of filing to all registered parties.

s/ Amy Strickling
Paralegal
Federal Public Defender Office

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710